ABSTRACT

The applicants have recognized an alternate method of performing modular reduction that admits precomputation. The precomputation is enabled by approximating the inverse of the truncator *T*, which does not depend on the scalar.

The applicants have also recognized that the representation of a scalar in a τ-adic representation may be optimized for each scalar that is needed.

The applicants have further recognized that a standard rounding algorithm may be used to perform reduction modulo the truncator.

In general terms, there is provided a method of reducing a scalar modulo a truncator, by pre-computing an inverse of the truncator. Each scalar multiplication then utilizes the pre-computed inverse to enable computation of the scalar multiplication without requiring a division by the truncator for each scalar multiplication.